2017 METŲ IV KETVIRČIO CERT-LT VEIKLOS ATASKAITA

Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2017 m. IV ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 12 960 pranešimų apie incidentus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų.**

Pažymėtina, kad 14,4 proc. pranešimų apie incidentus (arba 1 866) buvo detaliai tiriami CERT-LT specialistų. Daugiausia tai – svetainių klastojimo atvejai, paslaugų trikdymo atakos bei kiti išskirtiniai atvejai, įskaitant incidentus, apie kuriuos pranešta mūsų interneto svetainėje užpildžius specialią formą arba elektroniniu paštu. Likusioji pranešimų apie incidentus dalis apdorota automatiniu būdu, perduodant informaciją apie incidentą bei rekomendacijas paslaugų teikėjams, kuriems priklauso su incidentu susiję IP adresai. Palyginti su 2016 m. IV ketv. (13 874 incidentai), incidentų sumažėjo 6,6 procento. Palyginti su 2017 m. III ketvirčiu (13 281 incidentas), incidentų sumažėjo 2,4 procento.

Apie penktadalį visų incidentų (arba 2 606 pranešimai) sudarė kenkimo programinė įranga: virusai (įskaitant išpirkos reikalaujančius arba *ransomware*), Trojos arkliai, kirminai ir kitoks žalingas kodas. Tokių incidentų buvo 10 proc. mažiau nei 2016 m. IV ketvirtyje ir apie 13 proc. mažiau nei praeitame ketvirtyje. Dažniausiai žalingas kodas platinamas per interneto svetaines ir su brukalu (angl. *spam*), t. y., pasinaudojant socialine inžinerija bandoma įtikinti naudotojus atsidaryti laiško priedą, iš pirmo žvilgsnio nekeliantį jokios grėsmės aukos kompiuteriui.

Su pavojinga programine įranga betarpiškai susijęs kitas incidentų tipas – informacinių sistemų užvaldymai. Jų buvo 2 510, kone penktadaliu mažiau nei 2016 m. IV ketvirtyje. Paminėtina, kad nuo aptariamojo ketvirčio pradžios stebime padidėjusį užvaldytų svetainių panaudojimą kriptovaliutoms generuoti. Užuot užkrečiant lankytojų įrenginius kenkimo kodu (kaip tai buvo daroma anksčiau), dabar svetainių lankytojų kompiuteriai (arba išmanieji įrenginiai) vis dažniau išnaudojami lankytojams nenaudingiems skaičiavimams vykdyti.

Per šį ketvirtį buvo užfiksuoti 264 populiarių svetainių (pvz., *paypal.com*, *facebook.com* ir pan.) klastojimo atvejai, kone dvigubai daugiau nei prieš metus. Apie 90 proc. klastočių buvo pašalinta per 1 dieną. Buvo keli Lietuvoje veikiančių bankų el. bankininkystės svetainių klastojimo atvejai. Bendro pobūdžio populiarios lietuviškos svetainės šį ketvirtį nebuvo klastojamos.

Kiti ketvirčio įvykiai ir tendencijos (taip pat žr. naujienų skiltį):

1) Bent 20 kartų padaugėjo svetainių, kurios be lankytojo žinios generuoja kriptovaliutą, panaudodamos lankytojo įrangos skaičiavimo pajėgumus. Tarnybos nuomone, tokia veikla yra neetiška.
2) Aptariamą ketvirtį kur kas dažniau nei anksčiau buvo taikoma sukčiavimo kilnojamo turto (fotoaparatų, nešiojamų kompiuterių ir pan.) pardavimo sferoje. 2 tokios schemos požymiai: klastotas laiškas iš neva „PayPal“ ir prašymas pervesti tam tikrą pinigų sumą per „Western Union“.
3) Šventiniu laikotarpiu daugėjo netikrų elektroninių parduotuvių, kurių tikslas – išvilioti patiklių žmonių pinigus ar duomenis.
4) Apgaulingi el. laiškai, kuriuose prisistatoma įmonės vadovu ir pavaldinys prašomas atlikti „skubų pavedimą“ (angliškai tai vadinama *C-level fraud*), ir toliau buvo aktyviai platinami. Lietuvoje yra ne viena bendrovė, kurios darbuotojai buvo apgauti tokiu būdu. Piniginius srautus valdantys asmenys (pvz., buhalteriai) turi būti budrūs.

Žemiau pateikiame incidentų suvestines. Visas CERT-LT apdorotų incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.html. CERT-LT skelbia įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas socialiniame tinkle „Twitter“, ir norintys gali prisijungti (angl. *follow*) prie mūsų paskyros. Surikiuotos pagal temą rekomendacijos pateikiamos https://www.cert.lt/rekomendacijos.html.

1 lentelė. CERT-LT 2016 m. IV, 2017 m. III ir IV ketv. apdorotų incidentų skaičiaus palyginimas

Incidentų tipas	**Incidentų skaičius**			**Pokytis, proc.**	
	2016 IV	**2017 III**	**2017 IV**	**2017 IV / 2016 IV**	**2017 IV / 2017 III**
Kenkimo programinė įranga	2 989	2 898	2 606	-12,8	-10,1
Informacinių sistemų užvaldymas	3 098	2 704	2 510	-19	-7,2
El. paslaugų trikdymas	4	11	20	+400	+81,8
El. duomenų klastojimas	143	257	264	+84,6	+2,7
Vientisumo pažeidimai	1	4	2	+100	-50
Įrenginių saugumo spragos	5 801	6 392	6 362	+9,7	-1,6
Įvairaus pobūdžio	1 838	943	1 196	-35	+26,8
Iš viso	13 874	13 281	12 960	-6,6	-2,4

1 pav. 2017 m. IV ketvirtį CERT-LT tirtų incidentų diagrama (proc. nuo 100)